REMARKS

Claims 1-12 and 14-26 are pending in the application. Applicant reserves the right to pursue the original claims and other claims in this and other applications.

Claims 1, 6-8, 14-20 and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 7,024,553 to Morimoto in view of U.S. Patent 6,055,314 to Spies, et al. ("Spies"). This rejection is respectfully traversed.

Claim 1 is directed to a method of updating and using an encryption key used by a wireless station for encrypted communications with a wired portion of the network, and recites "physically separating from said wireless station a network communications device; physically connecting said separated network communications device to an encryption key updating device which is connected to a wired portion of said network, said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device; replacing an existing encryption key in said network communications device with a new encryption key from said generator sent over said wired portion of said network; physically reconnecting said network communications device containing said new encryption key with said wireless station of said network; and accessing said new encryption key on said network communications device during an encrypted communication."

As the Office admits, Morimoto does not teach or suggest at least "physically separating from said wireless station [the] network communications device; [and] physically connecting [the] separated network communications device to an encryption key updating device which is connected to a wired portion of said network, said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device." (Office Action, pg. 3). Indeed, Morimoto, which is directed to a *wireless* means of updating WEP keys, specifically teaches that "each of STAs 103 memorizes and supervises ... [new] encrypted key[s] delivered from the key management server 101 [*wirelessly*] *through* the AP 102 and has communication with the AP using the encrypted key[s]." (Morimoto, col. 7, lns. 62—col. 8, ln. 5, emphasis added). In other words, Morimoto *explicitly teaches away* from the concept of *physical* attachment of a *separated* network

communications device to a *wired* encryption key updating device (which is not an access point) for encryption key distribution, as recited by claim 1. Accordingly, even if Spies taught "physically separating from said wireless station [the] network communications device; [and] physically connecting [the] separated network communications device to an encryption key updating device," which as explained below, it does not, combination of the references would be improper.

Applicant submits that Spies, which is directed to a method for secure purchase and delivery of video programs, cannot cure the deficiencies of Morimoto even *if* the references could be combined. First, Spies is not in an analogous art as the Office suggests. (Office Action, pg. 3). Second, Spies merely teaches distributing *decryption* keys on removable IC cards (*e.g.*, PCMCIA cards) to enable a video player to decode video content stored on a DVD or other medium—Spies' IC cards are not *network communications devices*, nor do they provide "encryption key[s] used by a wireless station for encrypted communications with a wired portion of the network." (Spies, Abstract, col. 6, lns. 19-33). In fact, Spies teaches or suggests *nothing* of *network* encryption, much less "physically separating from said wireless station [a] network communications device; [and] physically connecting [the] separated network communications device to an *encryption* key updating device," as recited in claim 1. Spies' teachings are limited to discrete decryption of video content. Accordingly, claim 1 is believed to be allowable over the Morimoto and Spies combination.

Claims 6-7 depend from claim 1 and are believed to be allowable for at least the same reasons, as well as on their own merit.

Claim 8 recites similar limitations to claim 1, namely "a wireless network communications device containing [an] encryption key, said wireless station configured to access said encryption key on said wireless network communications device during said encrypted communications, said wireless network communications device being physically disconnectable from said wireless station and physically connectable to [a] wired encryption key updating device wired to said network to receive, store, and use a new encryption key which is configured to be transmitted over said wired network by said wired network communications device," and is

believed to be allowable over the Morimoto and Spies combination for at least the same reasons as claim 1, as well as on its own merit.

Claim 14 depends from claim 8 and is believed to be allowable for at least the same reasons, as well as on its own merit.

Claims 15, 17 and 20 also recite similar limitations to claim 1, namely "said wireless network communications device being physically removable from said station and storing an updateable encryption key used in conducting encrypted wireless communications from said wireless network station, said removable wireless network communications device being physically connectable to a wired network to receive, store, and use a new encryption key, said wireless station configured to access an encryption key on said wireless network communications device during a wireless communication," (Claim 15), "a storage area on said network card which stores an updateable encryption key for use by a wireless station when conducting encrypted wireless network communications, said encryption key being updateable when said card is physically connected to a wired network card interface which supplies a new encryption key, said wireless station configured to access said new encryption key on said wireless network communications device during a wireless communication," (Claim 17), and "a programming device connected to said wired network for receiving over a wire connection a new encryption key from said generator, said programming device being adapted to physically receive a wireless network communications device containing an updatable encryption key and storing said received encryption key in said wireless network communications device, said new encryption key on said wireless network communications device being accessible by a wireless network device during encrypted communications," (Claim 20), and are believed to be allowable over the Morimoto and Spies combination for at least the same reasons as claim 1, as well as on their own merit. Claims 16, 18-19 and 26 depend from claims 15, 17, and 20 respectively, and are likewise allowable.

Accordingly, Applicant respectfully requests that the rejection be withdrawn and the claims allowed.

Claims 2-3, 9-10, and 21-23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Morimoto in view of Spies and in further view of U.S. Pat. No. 4,369,332 to Campbell, Jr. ("Campbell"). This rejection is respectfully traversed.

Claims 2-3, 9-10 and 21-23 depend from claims 1, 8 and 20, and are allowable over the Morimoto and Spies combination for at least the same reasons discussed above with respect to claims 1, 8 and 20. Campbell, which is cited by the Office as teaching encryption key regeneration at specific or user-defined intervals, cannot cure the deficiencies of Morimoto and Spies discussed above. (Office Action, pg. 8). Accordingly, Applicant respectfully requests that the rejection be withdrawn and the claims allowed.

Claims 4-5, 11-12 and 24-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Morimoto in view of Spies and in further view of U.S. Pat. No. 6,226,750 to Trieger ("Trieger"). This rejection is respectfully traversed.

Claims 4-5, 11-12 and 24-25 depend from claims 1, 8 and 20, and are allowable over the Morimoto and Spies combination for at least the same reasons discussed above with respect to claims 1, 8 and 20. Trieger, which is cited by the Office as teaching comparison of newly-generated encryption keys to previous keys to ensure there is no repetition, cannot cure the deficiencies of Morimoto and Spies discussed above. (Office Action, pg. 8). Accordingly, Applicant respectfully requests that the rejection be withdrawn and the claims allowed.

In view of the above, Applicant believes the pending application is in condition for allowance.

Dated: May 18, 2009

Respectfully submitted,

By #41,198

Thomas J. D'Amico
Registration No.: 28,371
Matthew B. Weinstein
Registration No.: 62,202
DICKSTEIN SHAPIRO LLP
1825 Eye Street, NW
Washington, DC 20006-5403
(202) 420-2200
Attorneys for Applicant